Journal of Law and the Biosciences, 1–12
doi:10.1093/jlb/lsaa075
Original Article

Data privacy considerations for telehealth consumers amid COVID-19

Sharon Bassan

School of Law, Depaul University, Chicago, IL, USA
Corresponding author. E-mail: sbassan@depaul.edu

ABSTRACT

The COVID-19 emergency poses particularly high infection risks in a clinical setting, where patients and health care providers are placed in the same room. Due to these risks, patients are encouraged to avoid clinics and instead use Telemedicine for safer consultations and diagnoses. In March, the Office for Civil Rights (OCR) at the U.S. Department for Health and Human Services (HHS) issued a notice titled *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (the 'Notification'). The Notification relaxes the enforcement of privacy and security safeguards established by the Health Insurance Portability and Accountability Act (HIPAA) until further notice, in order to facilitate the transition to telehealth services for the broader purpose of promoting public health during the pandemic. Specifically, covered healthcare providers can use telehealth to provide all services that, in their professional judgment, they believe can be provided through telehealth. If providers make good faith efforts to provide the most timely and accessible care possible, they *will not* be subject to penalties for breaching the HIPAA Privacy, Security, and Breach Notification Rules. This paper examines the implications of the Notification on patients' health information privacy. It recommends that patients should undertake a careful reading of provider privacy policies to make sure their protected health information (PHI) is not at risk before switching to telehealth consultation. Acknowledging the limitations of patient self-protection from bad privacy practices when in need for medical treatment during pandemic, the paper proposes that consumers' data privacy should be protected through one of two alternative regulatory interventions: the FTC's authority under §5, or HIPAA's business associates agreements.

KEYWORDS: Covid-19, health information, privacy, public policy, telehealth

I. INTRODUCTION

The present COVID-19 pandemic has been declared a national public health emergency in the United States. While efforts are being made to 'slow the spread' in social settings, the virus poses particularly high infection risks in a clinical setting, where patients, doctors, and other health care providers are placed in the same room together. Due to these risks, patients are encouraged to avoid coming to clinics and instead use Telemedicine for safer consultations and diagnoses.

In a February bulletin, the OCR at the U.S. Department of HHS stressed that covered entities could not set aside privacy and security safeguards established by HIPAA during an emergency. Subject to few exceptions, the OCR emphasized that covered entities should continue operating in compliance with the law and that sanctions are still in place despite the COVID-19 outbreak.[1]

In March, the OCR reversed the February policy in issuing a *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* ('Notification').[2] According to the Notification, covered healthcare providers can use telehealth to provide all services that, in their professional judgment, can be provided through telehealth.[3] If health care providers make good faith efforts to provide the most timely and accessible care possible to patients, they *will not* be subject to penalties for breaching the HIPAA Privacy, Security, and Breach Notification Rules.

A departure from HIPAA privacy protections to the conventional legal protections for information transmitted by telecommunication and technology companies is significant in the United States, which does not have a federal data privacy law. The OCR's enforcement waiver rolls data privacy responsibility onto individual users. Yet, there are limitations to users' self-protection of privacy and policymakers must act. Next, the paper examines the Notification's implications for patients' health information privacy. It first lays out HIPAA's protections and their scope in regular time and then reviews the changes in protection during public health crisis.

II. HIPAA DATA PRIVACY PROTECTIONS

Under HIPAA, health information should be protected, whether collected for purposes of individual care or epidemiology and public health.[4] HIPAA's main goal is to ensure that patients' individually identifiable health information is properly protected according to national standards, while still allowing the flow of health information necessary to provide high quality health care and promote public health.[5] HIPAA protects data within the health system primarily through the Privacy and Security Rules.

---

1 Office for Civil Rights, *Bulletin: HIPAA Privacy and Novel Coronavirus* https://www.hhs.gov/sites/default/files/february-2020.pdf (accessed April 11, 2020).

2 Office for Civil Rights, *Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency*, https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (accessed April 11, 2020) [hereinafter: *the Notification*].

3 Office for Civil Rights, *FAQs on Telehealth and HIPAA during the COVID-19 Nationwide Public Health Emergency,* https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf (accessed April 11, 2020).

4 42 U.S.C.A. § 1320d(4)(A). Under HIPAA, 'health information' is information created or received by a health care provider, health plan, public health authority, and employer.

5 Office for Civil Rights, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (accessed April 11, 2020).

II.A. Standards for Privacy of Individually Identifiable Health Information ('Privacy Rule')

The Privacy Rule requires an individual's authorization—i.e., signed permission—to allow a covered entity to use or disclose their PHI.[6] At minimum, a valid authorization must contain the following core elements: a description of the information to be used or disclosed, identification of persons authorized to make the requested use or disclosure, identification of the those to whom the covered entity may make the disclosure, a description of each purpose of the disclosure, and an expiration date with respect to each purpose.[7] While not a classic informed consent, the process of obtaining an authorization should inform individuals in advance about how their information will be used or disclosed.

II.B. The Security Rule

The Security Rule requires covered entities to use appropriate administrative, physical, and technical safeguards to protect 'the confidentiality, integrity, and security of electronic protected health information' (e-PHI) that they create, receive, use, maintain, or transmit.[8] The rules surrounding safeguards are designed to be flexible and scalable so that a covered entity can implement policies, procedures, and technologies that are 'appropriate' for its particular size and capabilities. HIPAA is a multifaceted law, but a major principle that underlies its safeguards is the 'minimum necessary' standard. This standard requires covered entities to request, use, and disclose PHI to the minimum extent necessary to complete a task.[9]

II.C. Application to Business Associates

HIPAA also establishes requirements for covered entities with respect to their business associates (e.g., lawyers, accountants, billing companies, and other contractors) if their relationship entails creating or sharing PHI. Liability for business associates' HIPAA violations has led to efforts to develop comprehensive contracts known as Business Associate Agreements (BAA). The purpose of a BAA is to obtain a written assurance that business associates protect health information through compliance with HIPAA. According to the Security Rule, when service vendors not otherwise covered by HIPAA are 'business associates', their BAA should impose specified written safeguards on the PHI used or disclosed.[10]

---

6 45 C.F.R. § 164.508 (a)(1) (2007); *see* 45 C.F.R. § 164.502(a). A covered entity may not use or disclose protected health information, except either (1) as permitted or required by the Privacy Rule or (2) as the individual who is the subject of the information authorizes in writing.

7 45 C.F.R. § 164.508(c)(1).

8 Office for Civil Rights, *Summary of the HIPAA Security Rule*, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed April 11, 2020). Most measures are technological, e.g., access control tools (passwords and PINs to limit access only to authorized individuals), encryption (permitting access only individuals who can decrypt the system using a key to read the information), and audit trail features (records access history). Other measures include checksum, double-key, message authentication and digital signatures to ensure digital integrity. *See* 45 C.F.R. §160.103(4). *See also* Travis Murdoch and Allan Detsky, *The Inevitable Application of Big Data to Health Care*, 309 JAMA 1351, 1352 (2013) (suggesting extension of security measures similar to those used for PHI into other sectors to protect confidential financial data).

9 *Bulletin*, *supra* note 1.

10 45 C.F.R. §§ 164.502(e), 164.504(e); *see* 45 C.F.R. § 160.103. Business associates' functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. Business

The COVID-19 outbreak makes compliance with HIPAA increasingly difficult. However, HIPAA accounts for such situations by including relaxed standards that apply during public health emergencies, which are discussed next.

III. HIPAA PROTECTIONS DURING A PUBLIC HEALTH CRISIS

Because public health is a national priority, allowing access to data for public health activities is sometimes justified on policy grounds.[11] In this context, policymakers find that the interest of society outweighs individual privacy concerns. Monitoring and controlling the COVID-19 pandemic, and contagious diseases generally, falls squarely within the specified public health purposes envisioned by the drafters of HIPAA. Public health authorities respect the confidentiality of PHI, and the federal government and a majority of states have laws that govern the use of identifiable information they collect.[12] The OCR's Notification further softens HIPAA requirements for the purpose of promoting telehealth amid the COVID-19 outbreak.[13]

III.A. HIPAA Exceptions for Public Health Activities

The Privacy Rule expressly permits the use and disclosure of PHI without authorization for specified public health purposes.[14] It permits (but not requires) covered entities to share PHI with a public health authority without authorization 'for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease' and 'public health surveillance, public health investigations, and public health interventions'.[15] Furthermore, covered entities may use or disclose PHI to notify individuals 'who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease', or if such notification is authorized by law and necessary to conduct a 'public health intervention or investigation'.[16] The rule also permits covered entities to disclose PHI to foreign government agencies acting in collaboration with a public health authority.

Other public policy-based HIPAA exceptions could possibly apply to permit use and disclosure of PHI during COVID-19. Although additional requirements apply, a covered entity is permitted to use and disclose PHI as required by law (limited to the relevant requirements of that law); for health oversight activities authorized by law; for research purposes (provided the study comports with certain conventions); to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[17] Additionally, de-identified, aggregated data—such as a symptom heat

associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

11 45 C.F.R. § 164.512(b)(1)(i).

12 For the Center for Disease Control (CDC) report that helps public health agencies and others understand and interpret their responsibilities under the Privacy Rule, *see* CDC, *HIPAA Privacy Rule and Public Health—Guidance from CDC and the U.S. Department of Health and Human Services*, https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm (accessed April 12, 2020).

13 Office of Civil Rights, *FAQ*, *supra* note 3.

14 45 C.F.R. § 164.502(a)(1); W. Nicholson Price & I. Glenn Cohen. *Privacy in the Age of Medical Big Data*, 25 Nature Medicine 37, 41 (2019) (HHS allowed wide data sharing to promote 'key public goals such as research, public health, and law enforcement.').

15 45 C.F.R. § 164.512(b)(1)(i).

16 45 C.F.R. § 164.512(b)(1)(iv)

17 *See* 45 C.F.R. § 164.512(a)-(l).

map—is not considered protected under HIPAA, and even in normal times can freely be transferred.[18]

In the health care context, OCR's March Notification has recognized a new exception—at least temporarily—to counter the effects of COVID-19. During the public health emergency caused by COVID-19, privacy protections under the Notification diverge significantly from those under HIPAA. Although these measures may be necessary to ensure public health, individual consumers should be aware of the privacy risks they pose.

III.B. The Notification: Relaxed Enforcement for Telehealth

The Notification relaxes HIPAA's standards and further soften HIPAA protections to promote public health. Pursuant to the Notification, covered healthcare providers can provide telehealth services without being subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules.[19] HHS defines telehealth as 'the use of electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education, and public health and health administration'.[20] Technologies include videoconferencing, the internet, asynchronous imaging, streaming media, landline, and wireless communications. Using these technologies, telehealth may be provided through audio, text messaging, or video communication, among other means. Although relaxed enforcement applies regardless of whether telehealth treatment is for COVID-19 or other conditions, the Notification does not affect application of HIPAA outside the area of telehealth. [21] The Notification only applies to health care providers (not to all covered entities) in a telehealth setting. [22]

Some technology vendors have previously entered into BAAs, and, if they are familiar with the Security Rule, may have enhanced security capabilities. Others have not. The Notification includes vendors that market HIPAA-compliant video communication products, such as Skype for Business, Microsoft Teams, Zoom for Healthcare, and Google G Suite. However, OCR clarifies that it has not reviewed BAAs offered by these vendors, and this list does not constitute an endorsement of specific technology, software, applications, or products.

The practical purpose of this policy is to pardon health care providers if the manner in which they use technologies, or the technologies themselves, do not fully comply with the more stringent HIPAA requirements that usually apply. For example, they may not be encrypted or secure.[23] OCR, under the Notification, will not

18 45C.F.R.§164.528(a)(1)(viii).

19 Guidance addressing special data protection issues amid Coronavirus also exists in other countries. *See* Hogan Lovells, *Coronavirus and Data Protection—Guidance by Data Protection Authorities*, https://www.hoganlovells.com/media/pdf/2020PDFs/2020_03_20_Coronavirus (accessed April 11, 2020).

20 Office of Civil Rights, *FAQ*, *supra* note 3.

21 Office of Civil Rights, *FAQ*, *supra* note 3.

22 *The Notification*, *supra* note 2. A provider is a person or organization who furnishes, bills, or is paid for health care in the normal course of business, e.g., physicians, nurses, clinics, hospitals, home health aides, therapists, mental health professionals, dentists, pharmacists, and laboratories. By contrast, a health insurance company that merely pays for telehealth services would not be covered by the Notification.

23 Stanley Crosley, *Why the New HIPAA Telehealth Announcement is a Welcome Move*, https://iapp.org/news/a/telehealth-announcement/ (accessed April 11, 2020).

necessarily penalize providers without a BAA in place for telehealth purposes.[24] Although the Notification significantly alters ordinary HIPAA standards, OCR has designated certain 'public-facing' communication products (such as Facebook Live, TikTok, or chat rooms like Slack) as unacceptable for telehealth. These products create more risk than necessary because they are designed to be open to the public or allow wide or indiscriminate access to the communication. They do not follow the 'minimum necessary' principle. The Notification restricts telehealth products to 'non-public facing' remote communication products that, by default, allow only the intended parties to participate in the communication.[25] These telehealth providers are assumed to be more trustworthy in protecting patient PHI. But this trust is generally misplaced.

IV. IMPLICATIONS OF THE NOTIFICATION FOR DATA PRIVACY

Following the Notification, a substantial amount of health information (and consumer information more generally) that flows through remote communication technologies and health apps is not currently covered by HIPAA.[26] An upward trend in remote care will give a combination of public and private actors greater ease of access to electronic health information, creating uncertainty regarding applied legal protections. Lacking legal protections, consumers now must undertake a fine-grained analysis of provider telehealth privacy provisions in an attempt to figure out what risks are involved in telehealth and whether the convenience is worth the risks.

IV.A. Privacy Protections for Telehealth Technologies

HIPAA's scope is limited to covered entities (such as health plans and health care providers) who transmit PHI in electronic form in relation to health care treatment and transactions.[27] HIPAA's application to covered entities requires them to take responsibility with respect to using compliant technologies. However, telehealth apps that collect data directly from the consumer are not covered entities.[28] Hence, as providers transition to other custodians of the data, such as technology and telecommunication companies—even those that provide health-related commodities and services—data becomes unprotected under HIPAA. Meaning, the data may be equally sensitive, but information or analytics derived from sources not subject to HIPAA is not legally protected by HIPAA safeguards.[29] For example, consider a doctor who uses a company such as Facebook's online video and chat platform to consult with patients. Notably,

24 *The Notification*, *supra* note 2.

25 Office of Civil Rights, *FAQ*, *supra* note 3. 'Non-public facing' remote communication products would include, e.g., FaceTime and video chat and messaging using Facebook Messenger, Google Hangouts, WhatsApp, Zoom, or Skype. Other common texting apps such as Signal, Jabber, WhatsApp, or iMessage also fall within this category. These platforms are considered non-public because they typically use end-to-end encryption, which allows only the person with whom an individual is communicating to see the information transmitted. Many of these platforms also support safeguards such as individual user accounts, logins, and passcodes, and allow users to exercise some degree of control over their privacy settings, such as choosing to record or not record the communication or to mute or turn off video or audio at any point.

26 Natasha Lomas, *What are the Rules Wrapping Privacy During COVID-19?*, https://techcrunch.com/2020/03/20/ (accessed April 11, 2020).

27 45 C.F.R. § 164.306(a).

28 *Id.*

29 Kevin Coy and Neil Hoffman, *Big Data Analytics Under HIPAA*, https://www.jdsupra.com/legalnews/big-data-analytics-under-hipaa-80678/ (accessed April 11, 2020).

care may be delivered by a professional that is ordinarily subject to HIPAA, but the health information provided through Facebook may be regulated under Facebook's privacy policy, and therefore subject to relaxed standards.

Lacking legal protection, the default legal scheme for any information transmitted and gathered through telehealth technologies during the time that the Notification applies is the company's 'Privacy Policy' or 'Terms of Conduct'. Privacy policies design the relationship between data subjects and data holders and specify the company's management of data. It shapes the legal and ethical requirements that an entity self-imposes when collecting, using, and sharing health data. To ensure they can access the platform, consumers must surrender to the company's privacy policy without being able to ex post facto void the terms of service.

Effectively, since there is no comprehensive legislation to monitor telehealth technologies that are not covered by HIPAA, telecommunication companies can gather health-related information as they wish.[30] Everything not specifically mentioned is open to interpretation.[31] If government and industry leaders were more attentive to legality, security, and privacy in the run up to the COVID-19 crisis, consumers could embrace new remote health measures that have been deployed with confidence. Unfortunately, this is not the case.[32] It is unlikely that privacy policies will adapt according to new telehealth use. On the contrary, companies will most likely leverage information legally gathered during this time.[33] Health information accumulated in time of pandemic is highly valuable for those who profit based on it: health providers, health and medical device vendors, health insurance companies, health devices manufacturers, pharmaceutical companies, telecommunication and technology companies whose products may be used to provide telehealth, and advertisers.

If privacy policies do not provide otherwise, this information would not be deleted—it could be stored, used, and possibly sold to third parties. In addition to its commercial value, users' information can feed intelligence and policing, being highly useful for enforcement. Consistent with their privacy policies, companies often use information for their business purposes, or disclose or sell information that they hold with third parties. For example, Zoom, one of the most popular platforms being used today, updated its privacy policy in March after a report revealed that its terms would have allowed the company to collect user information, including meeting content, and analyze it for targeted advertising or other marketing.[34] The OCR encourages providers to notify patients that third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when

30 Angela Chen, *Why it's Time to Rethink the Laws that Keep Our Health Data Private*, https://www.theverge.com/2019/1/29/18197541/ (accessed April 11, 2020).

31 David Hill, Data Protection: Governance, Risk Management, and Compliance (2016).

32 Privacy International, *Covid-19 Response: Overview of Data and Technology*, https://privacyinternational.org/key-resources/3547/ (accessed April 11, 2020).

33 *See* Lily Hay Newman, *The Zoom Privacy Backlash Is Only Getting Started*, https://www.wired.com/story/zoom-backlash-zero-days/ (accessed April 22, 2020). (Zoom had a reputation for prioritizing ease of use over security and privacy. The company is facing a class action lawsuit over the data its iOS app sent to Facebook.)

34 *Id.*

using such applications.[35] Yet, each company is limited only according to its own privacy policies.

Rather than HIPAA, technology and telecommunication companies are subject to commercial law and enforcement by agencies such as the Federal Trade Commission (FTC). The FTC protects consumers from unfair trade practices through regulation and enforcement of various laws.[36] It can bring actions against companies for being misleading or deceptive, but typically does so only in extreme circumstances.[37] Companies that violate their own privacy polies may be subject to enforcement for misleading consumers. However, if a company has set lax standards or its privacy policy includes a notification that it will widely disseminate user data, there is little that the FTC can do to protect those who have accepted it.[38] Even questionable use of personal information does not necessarily mandate enforcement.[39] At the moment, by providing these notices and fulfilling their contract, companies who are data owners comply, at least formally, with their obligations.[40]

IV.B. Consumers' Responsibility Before Using Telehealth Technologies

This new reality puts health care consumers in an unusual situation. Given the OCR's waiver of typical enforcement standards, consumers are now solely responsible for their data privacy protections, or lack thereof. The ball is in the court of patients who use telehealth to take precautions before switching to online consultation. When engaging in telehealth, reading the privacy policy of whichever technology one decides to use can be considered best practice. Given that consumers cannot ex post facto void the terms of service based on their failure to read or understand the policy, it is highly recommended for patients to spend time doing so with respect to any technologies that they consider using during the COVID-19 outbreak.

In this respect, both HIPPA and state laws such as the California Consumer Privacy Act (CCPA) specify certain information for which users should keep an eye out. The core elements for obtaining an authorization under HIPAA's Privacy Rule can be useful starting points. These elements stipulate the specific information to be used or disclosed, persons authorized to use or disclosure the information, those to

35 Office of Civil Rights, *FAQ*, *supra* note 3.

36 Federal Trade Commission, *What We Do*, https://www.ftc.gov/about-ftc/what-we-do (accessed April 11, 2020).

37 15 U.S.C. § 45(n). Unfair practices are defined as those 'likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'

38 Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 Penn. St. L. Rev. 777, 790 (2016) ('If users do not do their homework on what information their apps are collecting about them, and the app makers are not foolish enough to outright lie about what they are doing, the FTC's ability to control how companies share our data is very limited.').

39 Cal. Civ. Code § 1798.145 ('Sec. 2 The Legislature finds and declares that . . . (g) In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica . . . As a result, our desire for privacy control and transparency in data practices is heightened.').

40 *Tompkins v. 23andMe*, 2014 WL 2903752, addressed whether 23andMe's customers are bound by their site's Terms of Service (TOS), which include consent and privacy terms. The court held that as long as 23andMe provides notice of the terms by providing a link to access, review, and assent to the policies, notice is sufficient. The Court concluded that the plaintiffs accepted the TOS when they created accounts or registered their DNA kits. A consumer cannot ex post facto void the terms of the commercial sale of service based on his failure to read the terms.

whom disclosure may be made, and each purpose for disclosure.[41] Similarly, the CCPA specifies the information that should be identified in the privacy policy in order to protect consumers.[42] It could be classified to these three categories:

- Consumers' right to request information: a statement of consumers' right to request that the business disclose what personal information it collects, uses, discloses, and sells; ideally, instructions for submitting a verifiable consumer request and links to an online request form or portal for making the request; a general description of the process the business will use to verify the consumer request, including any information the consumer must provide.
- Information about data collection and management: the categories of personal information the business collects about consumers, from which categories of source personal information is collected.
- How the information will be used and shared: for each category of personal information identified, identification of the business or commercial purpose for collecting, disclosing or selling personal information with third parties; identification of the third parties to whom the information was disclosed or sold; statement of whether the business has actual knowledge that it sells the personal information of minors.

IV.C. Users' Self-protection Is an Unrealistic Expectation

Consumers (who are patients) have no choice but to be vigilant, but there are limits of data privacy responsibility that individual users can take under the circumstances of pandemic:

First, Individuals may be in a socially and/or financially vulnerable position due to the circumstances of COVID-19. Those seeking care because of COVID-19 infection need immediate medical counseling and treatment and cannot go out and risk others. In this position, they will probably be forced to use whatever technology their healthcare provider choses, for their own sake and for the public's benefit.

Second, although the ordinary consumer may not be accustomed to picking through privacy policies, the Notification requires them to exercise increased caution. However, privacy policies are often written in an unclear language and are rarely read.[43] I will be surprised if all privacy policies are clear and specific about how they handle information, even in this sensitive time. Moreover, consumers lack control and cannot negotiate privacy terms with telecommunication companies before using their platforms (for example, regarding use of the PHI they expose in telehealth technologies). [44] Rather, these companies have a 'take it or leave it' approach. Business incentives that the pandemic emergency introduces are not advantageous to consumers. It puts commercial entities in great advantage and enhances their marketing abilities. Thus, the risk of

41 45 C.F.R. § 164.508(c)(1).

42 California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.198(a), 999.308(c)(1).

43 *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, in Consumer Protection in the age of the 'Information Economy' 341; 360–61 (Jane K. Winn ed., 2006) (explaining that privacy policies are difficult to understand and that most Americans therefore do not read them).

44 Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks*, 27 Health Matrix 143, 145 (2017).

commercial exploitation is high. This is not a unique COVID-19 problem, but given the vulnerabilities caused by the pandemic, consumers are further impoverished.

Third, users' vulnerable position poses substantial risks to their information privacy in the long run, since some accumulated information may maintain its value years after the pandemic is over. It may be a long time before our health information is protected again; the OCR Notification does not have an expiration date. Instead, OCR will issue a notice to the public when it is no longer exercising its enforcement discretion based upon the latest facts and circumstances.[45] It is not in the hand of consumers' to prevent this long-term predictable and irreversible consequence.

Given those predictable vulnerabilities, the OCR reliance on consumer self-protection through reading the privacy policies is patently unrealistic. Such a responsibility should not be rolled over to consumers. It is in everyone's interest to incentivize patients to seek health care treatment rather than avoid doing so.

V. TWO ALTERNATIVE REGULATORY INTERVENTIONS

Understanding the importance of social distancing in times of pandemic, this paper does not discourage the use of telecommunication technologies. If possible, people who need treatment should get the care they need remotely, rather than going outside, risking exposure to infection and overwhelming clinics. Applying the public policy rationale, the risk of infection may well be higher than potential privacy risks. However, during this sensitive time, and amid increasing calls for better government leadership, consumers' data privacy should be protected. Regulation is therefore unavoidable.

In times of pandemic it may be impractical to suggest enactment of a law to address the privacy considerations involved with telehealth. However, there are two more flexible alternative regulatory interventions, one potential mechanism is through the FTC, and the other mechanism is through HIPAA's BBAs.

V.A. FTC's Authority Under §5

To date, the FTC's primary enforcement tool to deter unfair or deceptive privacy and data security practices is to serve offenders with cease and desist orders and consent orders pursuant to the Federal Trade Commission Act of 1914, as amended. The FTC cannot bring a civil action or recover penalties for unfair practices unless a company violates a final order. In the absence of effective privacy or data security programs, these remedial measures may provide limited incentive for companies to refrain from unfair practices until after they are caught and penalized the first time. In a recent ruling by the Eleventh Circuit Court of Appeals in *LabMD vs. FTC*, the Court stated that it is not the FTC's place to decide what specific controls a company should implement, but rather to evaluate whether those controls are sufficient to avoid unfair or deceptive practices.[46] In response, Representative James Langevin argued that the Court's decision may limit the FTC's ability to issue orders that specify desired outcomes in order to remedy unfair and deceptive data security practices (as compared to elaborating on specific controls).[47]

45 Office of Civil Rights, *FAQ*, *supra* note 3.

46 *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018)

47 Rep. James Langevin, Public Comment #FTC-2018-0052-D-0017, *Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201*, https://www.ftc.gov/system/files/filings/initiati

Moreover, unlike other unfair and deceptive business practices, negligent handling of consumer information can result in repeated, untraceable injuries that are far removed in time from the practice that caused the injury. Thus, Langevin recommended that the FTC should consider the criteria used to evaluate the § 5(n) standard of 'substantial injury to consumers' in the context of failures to implement reasonable data security or privacy practices. The FTC bears the burden of proof to demonstrate the potential for harm. If the Commission can show that sensitive data could be accessed by parties not authorized by the consumer, injury should be presumed. [48]

At the moment, the FTC is tracking complaint data related to COVID-19 and taking actions against scammers using the pandemic to deceive or defraud consumers.[49] According to FTC Chairman Joe Simons' statement on the agency's efforts to protect consumers during the pandemic, the FTC is working with enforcement authorities and other stakeholders to stop fraud and unfair and deceptive business practices: '[w]e will not tolerate businesses seeking to take advantage of consumers' concerns and fears regarding coronavirus disease, exigent circumstances, or financial distress'.[50] The FTC should clarify its position through orders addressing unfair practices and substantial injuries in the context of telehealth in times of the Coronavirus.

V.B. HIPAA's Business Associates Agreements

A second solution could be found under HIPAA. OCR and HHS are currently under a lot of pressure related to COVID-19 implications. OCR declared that it has not reviewed the BAAs offered by the vendors it recommended in the Notification, and therefore, the list does not constitute an endorsement, certification, or recommendation of specific technology, software, applications, or products.[51] Avoiding review and endorsement of specific BAAs seems unreasonable. OCR and HHS should have acted even during the first months of the pandemic because addressing telehealth privacy issues is an essential requirement: First, not only a timely, the long-term harms that telehealth entails for information that is usually considered PHI, and thus covered by HIPAA, are substantial, predictable, and inevitable unless addressed by regulation. Second, throughout the extended period of time that the U.S. has been on lockdown, the OCR has been addressing civil rights through announcements, notifications of enforcement discretion, and other guidance.[52] However, OCR and HHS have abdicated their regulatory responsibility in the case of telehealth and must act immediately. Given the implementation of the technology during the pandemic, it is unlikely that the use of telehealth would disappear after the pandemic. Now, after all the time that has passed since the Notification, the OCR must review privacy policies of recommended

---

ves/758/public_comment_from_representative_langevin_re_topic_5_redacted.pdf (accessed April 20, 2018).

48 *Id.*

49 FTC, *Coronavirus (COVID-19) Pandemic: The FTC in Action*, https://www.ftc.gov/coronavirus (accessed April 22, 2020).

50 FTC, *FTC Chairman Joe Simons Outlines the Agency's Approach to Safeguarding Consumers during the Coronavirus Pandemic*, https://www.ftc.gov/news-events/press-releases/2020/03/ftc-chairman-joe-simons-outlines-agencys-approach-safeguarding (accessed April 22, 2020).

51 *The Notification*, *supra* note 2.

52 Department of Health and Human Services, *HIPAA, Civil Rights, and COVID-19*, https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html (accessed April 22, 2020).

telecommunication platforms and endorse those that would pose minimal harm to patients' privacy.

Unlike many other rights, in a data-based world where machine learning is thriving, individuals' data privacy or lack thereof has long-term irreversible effect beyond the period of the pandemic. The ramifications of relaxed standard put individuals in an impoverished situation and require an immediate regulatory response. Without a BAA in place, patients who use telecommunication technologies are subject to companies' privacy policies. But BAAs' requirements significantly raise the costs and complexities of telehealth software investments.[53] Healthcare providers may be challenged in finding telehealth technology partners willing to sign BAAs in time of pandemic.[54] To encourage companies to subject their platforms to HIPAA's BAA's standards, the OCR should inform the public whether companies signed binding BAAs. Such an approach would incentivize platforms to comply with HIPAA, as it would be in companies' business interest to gain public credibility and trust that would encourage more consumers to adopt their technology and use their services.[55] Additionally, the FTC must ensure that some of the recommended platforms are free, so fees would not be an impediment to patients seeking care. This solution may be preferable to the FTC. First, it presents an ex ante, rather than ex post solution. Second, it is based on a market rationale and entails a commercial incentive for companies who comply.

This is not beyond, but rather an integral part of the emergency conduct needed in this time to prevent long-term privacy harms.

53 Mason Bernard, *Telehealth Policy and COVID-19: Expanding Access without Compromising Privacy*, Center for Democracy and Technology, https://cdt.org/insights/telehealth-policy-and-covid-19-expanding-access-without-compromising-privacy/ (accessed Sept. 22, 2020).

54 Shachar C, Engel J, Elwyn G, *Implications for Telehealth in a Postpandemic Future: Regulatory and Privacy Issues.* 323(23) JAMA 2375–2376 (2020). doi:10.1001/jama.2020.7943

55 For a supplementary suggestion for telehealth practitioner licensing, see also, Shachar C, Engel J, Elwyn G, *Implications for Telehealth in a Postpandemic Future: Regulatory and Privacy Issues.* 323(23) JAMA 2375–2376 (2020). doi:10.1001/jama.2020.7943